IN THE SPECIFICATION:

Please amend the paragraph at page 3, lines 3-4 as indicated in the following:

~~FIG. 5 is a block diagram~~FIGS. 5A and 5B are block diagrams illustrating dual link communications between a video controller and a display, according to one embodiment of the present invention.

Please amend the paragraph at page 4, lines 14-24 as indicated in the following:

Software public key 126 can be stored as a part of memory 120 and video driver 123. Software public key 126 and any necessary private keys 127 can also be loaded from a basic input/output system (BIOS) chip 125. Alternatively, software public key 126 and any necessary private keys 127 can be downloaded from a network, such as the Internet 170, through a communications interface 135. A_N is generated by video driver 123. The information handling system 110 may contain other devices such as an audio card (not shown), communications interface 135, etc. It will be appreciated that other internal bus types may be used, such as the Video Electronic Standards Association local bus (VLB), the industry standard architecture (ISA) bus, or the extended ISA (EISA) bus, without departing from the spirit or scope of the present invention.

Please amend the paragraph at page 8, lines 6-26 as indicated in the following:

Video controller 140 processes commands from video driver 123 and generates commands to display video on display 150 through a processing circuit 145. Video controller 140 receives the software public key 126 and the PRN generated by video driver 123. In one embodiment of the present invention, video controller 140 reads an upstream public key 166 and a set of upstream private keys 167 for communicating with video driver 123, from ROM module 149, through an integrated ROM interface 147. In accordance with one embodiment of the present invention, the keys stored on the ROM module 149 can be protected using a variety of protection schemes, including one described in a pending patent application having a client

docket number 000153BT, entitled "WRITE ONCE SYSTEM AND METHOD FOR FACILITATING DIGITAL ENCRYPTED TRANSMISSIONS", filed on November 2, 2000. Video controller 140 uses the set of upstream private keys 167, the monitor public key 156, a PRN generated for display 150, the driver public key 126 and the PRN received from video driver 123, to generate an authorization key for communicating with video driver 123, as described in the ~~enclosed~~ Upstream Link for HDCP Revision 0.95 specification. Video controller 140 transmits the upstream public key 166, the monitor public key 156, the PRN generated for display 150, and a concatenated version of the authorization key generated by video controller 140, to video driver 123, over PCI bus 137. Registers 141, 142, 143, 144, and 146 can be used to store the data received and generated by video controller 140, as previously discussed for FIG. 1.

Please amend the paragraph at page 12, line 26 to page 13, line 9 as indicated in the following:

In step 350, the video driver receives A_N, BKSV, S', and DKSV. In step 360, the values of BKSV, DKSV, A_N, along with the set of private keys associated with the video driver, are used to generate a key, Kp. By concatenating the value of Kp with the status data of the video driver, a value S can be generated. The calculations for generating Kp and S are similar to those described in the ~~enclosed~~ *Upstream Link for HDCP* specification. In step 370, the value of Kp can be compared to Kp', through the comparison of S with S'. If the values are equal, the video controller and the video driver can be considered successfully authenticated indicating that the status data is valid. If the values differ, video controller can decide to terminate communications with the video controller until it passes the authentication. In one embodiment, the values of Kp and Kp' are used for encrypting and validating the ~~authenticy~~ authenticity of communications over the PCI bus. In a specific embodiment, the status data of the ~~vidoe~~ video controller is checked at least every two seconds by the video driver to assure secure communication is maintained.

Please amend the paragraph at page 14, lines 6-10 as indicated in the following:

Referring now to ~~FIG. 5~~<u>FIGS. 5A and 5B</u>, a system for handling encrypted dual link DVI video data is shown, according to one embodiment of the present invention. A video controller 510, communicating with a digital video interface (DVI) display 560, generally queries display 560 to determine the capabilities of display 560. The capabilities of display 560 can be used to determine the amount of data sent by video controller 510.